# Security Indoctrination Brief

Our cleared companies have entered into a Common Security Services Agreement (CSSA) with the consent of the Defense Security Service. As part of this agreement, Akima has assumed the responsibility for security indoctrination and training required under the provisions of the National Security Information Program (NISP).

Based upon information provided by the Defense Security Service, you have been granted eligibility for access to classified information at a level commensurate with the investigative requirements and need to know. Prior to being granted access to classified information, you will be required to read this briefing in its entirety. At any time, if you feel that you require further clarification, you should contact any member of the security staff for further guidance. After you have read and acknowledged your understanding of its contents, you will be asked to complete a Standard Form 312 – National Security Non-Disclosure Agreement (SF312).

Once you have properly executed the SF312, provide the original to the company security office. As an interim measure, you may email or fax copies of the completed form to the security group. However, the originals must be forwarded to complete the record. Upon receipt the security group will make the appropriate entries in JPAS and submit visit requests as appropriate to the government. Your supervisor will be notified once all of the required security actions have taken place. We also recommend that you maintain a copy for your own records.

**YOUR SECURITY STAFF**

CONTENTS

# SECURITY INDOCTRINATION BRIEFING

## GENERAL INFORMATION

As Defense Contractors, we are required by the Defense Security Service (DSS), in accordance with our Security Agreement, to give a security indoctrination to all personnel before allowing them access to classified information. Your *individual* access may be limited based upon the required need-to-know. We are required to install and maintain comprehensive security measures for the protection of classified material developed by or furnished to us. It is the personal responsibility of every employee who handles, or otherwise comes in contact with classified information; to observe at all times our written company security procedures and other instructions as may be issued by the Security Office.

## NATIONAL INDUSTRIAL SECURITY PROGRAM (NISP) OVERVIEW

The NISP is the U.S. government / industry program to safeguard classified information that has been entrusted to industry in conjunction with defense contracts. This is a partnership, in which the government customer or Government Contracting Activity (GCA) enters into a classified contractual agreement with a cleared industrial facility. DSS – on behalf of the Department of Defense (DOD) - has been delegated the security administrative responsibilities for these classified contracts. This means that DSS will provide advice, assistance, and ensure compliance with all applicable requirements of the National Industrial Security Program Operating Manual (NISPOM) that affect our classified program(s). It does this by conducting regular security reviews at all cleared companies.

The NISP is commonly administered within each cleared facility by the Facility Security Officer (FSO). Top management is ultimately responsible for administration of the classified program, but this authority is generally delegated to the FSO. The FSO is responsible for all security matters relative to the safeguarding and handling of classified information.

The NISPOM is industry's primary reference in the protection of classified information. This manual outlines the proper procedures for handling and safeguarding information classified pursuant to Executive Order 12958, as amended. It provides uniform rules for all industrial companies under the NISP, and each company working on any government, classified contract must comply with its provisions.

DSS Industrial Security reviews are normally all encompassing and tend to include a review of the company's security procedures to include, if applicable, the Standard Practice Procedures (SPP), accredited information systems, classified visits, security education and safeguarding and handling of classified information. The level and amount of classified material that the company has in its possession normally determines the frequency and length of such reviews.

DSS has the authority to suspend or revoke a facility clearance if it finds that the company's security procedures are unsatisfactory for handling and safeguarding classified information. The DSS rating of unsatisfactory can negatively impact a company's ability to conduct future classified work. Consequently, poor security practices are not only detrimental to the national security, but they may have a direct impact on all employees' jobs and the company's ability to perform on classified contracts.

## CLASSIFIED INFORMATION DEFINITION AND DESCRIPTION

***Classified information*** is official government information that has been determined to require protection in the interest of national security. All classified information is under the sole ownership of the U.S. government, and as such employees possess no right, interest, title, or claim to such information. (One exception – information developed under an Independent Research & Development (IR&D) Program).

Classified information exists in many forms. It may be a piece of hardware, a photograph, film, recording tapes, notes, drawing, document or spoken words. Classified material is marked as such upon origination. It comes to

industry via a DD Form 254, security classification guides or classified source materials. The degree of safeguarding required depends on its classification category. Three levels of classification have been established based on their criticality to national security:

TOP SECRET: Information or material whose unauthorized disclosure could be expected to cause exceptionally grave damage to national security.

SECRET: Information or material whose unauthorized disclosure could be expected to cause serious damage to national security.

CONFIDENTIAL: Information or material whose unauthorized disclosure could be expected to cause damage to national security.

DSS has security cognizance over DOD classified information bearing any of these three classification levels. There are also other categories of classified information that require special access authorization. The customer will provide information concerning these. You may hear terms such as Sensitive Compartmented Information (SCI), or Special Access Program (SAP). Information pertaining to these programs will be provided if you are assigned to work with these programs.

***Sensitive But Unclassified Information:*** There are other categories of information, which, while not classified, deserve mention. For Official Use Only (FOUO), Sensitive But Unclassified (SBU) for example, is unclassified information which is exempt from general public disclosure and must not be given general circulation.

As a minimum, after the determination of the level of classification, classified material shall be marked with the date of origin, the name and address of the facility responsible for its preparation, and be plainly and conspicuously marked, stamped or typed with the appropriate classification level at the top and bottom of each page, front and back. Each portion, section, part, paragraph, or similar portion of a classified document shall be marked to show the level of classification.

***Proprietary Information:*** In addition to government classified information, the company produces a large amount of company private or proprietary information. This information is not to be divulged to individuals outside of the company. Examples of this information are salary and wage lists, technical and research data, trade secrets and proposals. Employees should protect this information in such a manner as to preclude unauthorized access. This information can be marked Company Confidential or Company Private. Caution should be taken to keep this information separate from U.S. government classified information.

## ACCESS REQUIREMENTS AND NEED-TO-KNOW

Access to classified information occurs when a person has the ability and opportunity to obtain knowledge of the classified information. Authorized access to classified information may be granted only when two conditions are met: First, the recipient must have a valid and current security clearance (***eligibility for access in JPAS***) at a level at least as high as the information to be released. Second, the recipient must demonstrate the need for access to the classified information. This is referred to as ***need-to-know***.

Need-to-know is met when access to classified information by an individual is essential to the performance of his or her job duties in fulfilling a classified contract. Each individual, regardless of rank, position, or amount of clearances and accesses, only has a need-to-know for information pertinent to the performance of his or her specific program. Need-to-know is not the same as want-to-know. Individuals must always establish a person's need-to-know before sharing classified information.

It is the responsibility of the holder of the classified information to ensure the proper clearance and need-to-know of the recipient. The possessor must also advise the recipient of the classification of the information disclosed.

Need-to-know confirmation should come from a security representative. If there is doubt as to whether or not a person has a need-to-know, the employee should check with the security representative prior to the release of any classified information. Establishment of need-to-know is critical. It is far better to delay release to an authorized person than to disclose classified information to an unauthorized individual.

## SAFEGUARDING CLASSIFIED INFORMATION

One of the most fundamental requirements of the NISP pertains to the proper safeguarding and storage of classified information. It is essential that classified information be properly safeguarded or stored in accordance with the requirements of the NISPOM at all times. A natural way of approaching the subject of safeguarding is to divide it into simple requirements for safeguarding while classified materials are in use and when not in use.

**WHILE IN USE**

While in use, classified material must never be left unsecured or unattended. An authorized individual who is able to exercise direct control over the classified material must keep it under constant surveillance. The authorized individual must have the appropriate clearance and need-to-know, and must take action to prevent access to the material when others who do not have the appropriate clearance and need-to-know.

When working with classified material in an unsecured area, any open doors should be closed. It is prudent to also post a sign, declaring "CLASSIFIED WORK IN PROGRESS". If a visitor or unauthorized employee is present, a classified document must be protected by either covering it, turning it face down, or placing it in an approved storage container.

When working on classified material you must lock the documents in an approved storage container when you leave your desk for any reason including lunch or coffee/smoke/bathroom breaks. They must never be tucked in a desk drawer, file cabinet, credenza, key-lock file, etc., for even the briefest period. If you are working on an approved computer and need to take a break, you must comply with the Information Systems (IS) procedures. You cannot just turn off your computer and expect the classified information to be safe. Classified information should be properly stored as soon as possible after it has been used.

**WHEN NOT IN USE**

When not in use, classified material must be properly secured in an approved security container, unless another properly cleared person with a need-to-know is guarding it. The storage of classified material in anything other than an approved container is strictly prohibited.

Approved storage containers must remain in a locked position unless they are under constant surveillance and control. The cleared employee should always shield the combination from the sight of others when opening a classified container. Combination padlocks must be stored inside or locked on the container when it is open. This prevents tampering or replacement of the padlock by an unauthorized person.

Combinations to classified storage containers and controlled areas are themselves classified and must therefore be protected at the same level of the information they are protecting. Combinations to classified containers must be committed to memory. They cannot be written on slips of paper to be kept in desks, wallets, notebooks, etc. In addition, they cannot be written down in a coded form, such as backwards, out of order, etc. In choosing a combination, employees should avoid persons, places or things that can be easily identified with them, such as a birthday, spouse's name, favorite sports team, license plate, etc. Only those employees authorized to have access to the container may know the combination. Whenever anyone with access leaves the organization or transfers to another group, the combination must be changed.

If circumstances prevent you from storing material in the prescribed container you should inform the FSO and hold the material until the FSO arrives and takes control of the material. The FSO will take the material to the security office for storage.

## TRANSMITTAL OF CLASSIFIED MATERIAL

The transmittal of classified material, ***when authorized,*** will generally be performed by the FSO. For questions concerning transmittal you should contact the FSO. No employee or visitor is allowed to bring classified material in or out of authorized facilities without the knowledge of the Security Office.

When classified storage is authorized, each cleared contractor within the cleared organization is required to maintain complete records for all classified material in its possession. All classified information will be logged into the Information Management System (IMS). For Top Secret, the FSO will be consulted prior to receipt. Special arrangements must be made for the transmittal and storage of Top Secret material.

Methods for transmittal of classified information depend on the material's classification and its destination. The FSO will ensure that the material is properly packaged, receipts included, and transmitted in accordance with the NISPOM.

## REPRODUCTION

Prior to reproducing any classified information, check with the FSO or your government on-site security representative. Each copy made must be entered into the IMS and all waste disposed of properly. Only certain copying machines are authorized for use. Additional information and procedures will be explained by the FSO at the time reproduction is required. Remember that the reproduction of classified information will be held to a minimum.

## DESTRUCTION

When it is determined that a piece of classified information is no longer required, it should be destroyed. Material to be destroyed will be done in a manner approved by DSS. A witness, while not required for material classified Secret or below, should be used. The destruction of Top Secret material requires a witness and a record for the destruction.

## EMPLOYEE REPORTING REQUIREMENTS

The NISP is based to a large extent on individual trust and responsibility, and employee reporting requirements are a critical element in the program. Employees are required to report any suspicious occurrences, known security infractions, adverse information and any change in employee status. Employee reporting requirements are designed to protect the employee and counter any possible hostile intelligence threat. It is your personal responsibility to understand and report these conditions to the FSO as circumstances warrant.

## SUSPICIOUS CONTACTS

Employees are required to report any suspicious behavior or occurrences that may occur at any time. More specifically, employees must report to the FSO any of the following events:

1. Any efforts, by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified or sensitive information.
2. Any efforts, by any individual, regardless of nationality, to compromise a cleared employee.
3. Any contact by a cleared employee with a known or suspected intelligence officer from any country.
4. Any contact, which suggests the employee concerned, may be the target of any attempted exploitation by the intelligence services of another country.
5. Any unsolicited attempts from any unknown person to get information about your company, to include its products and services and employees.

## SECURITY VIOLATIONS

Employees are required to report known or suspected security violations to the FSO. Reporting provides employees with an opportunity to extricate themselves from a compromising situation and enhances the protection of the national security information. Ideally, our security posture should be enhanced as the result of a security violation, because security professionals will have an opportunity to address and correct any problems that may exist. When an employee covers up a known security violation, the security education process is negated because security is denied the chance to rectify deficiencies. The relationship of mutual trust between the contractor and the DSS is also jeopardized. In addition, not reporting a known security violation may constitute a major security violation itself, regardless of the severity of the unreported incident. Some common security violations are:

1. Classified material left out or unattended.
2. Unsecured, unattended security containers/unsecured combinations.
3. Removal of material without approval.
4. Loss of classified information.
5. Unauthorized copying or destroying classified material.
6. Unauthorized/improper transmission of classified material.
7. Disclosure of/permitting access by an unauthorized person.
8. Processing classified material on a non-accredited computer.

## DISCIPLINARY GRADUATED SCALE ACTIONS

The company has established strict disciplinary action procedures for employees who knowingly and willingly violate the security procedures outlined in the Company SPP. Such actions will be coordinated with Human Resources and Company Management. Repeated violations of the security procedures may result in termination of employment. Some common examples of security violations are security containers left open and unattended; unsecured combinations; removal of classified material without approval, loss of classified information; copying or destroying classified material without approval; unauthorized/improper transmission of classified material; and disclosure of or permitting access to classified information to an unauthorized person.

***Progressive Disciplinary actions* may include, but are not limited to:***

First Instance: Verbal Counseling
Second Instance: Written Warning and Performance Improvement Plan
Third Instance: Final Written Warning

- *For Major Violations*

Same as minor violations and may include suspension/termination of employment
Loss of security clearance
Arrest
Imprisonment and/or fines

**Based on the violation, disciplinary action may not include all steps listed and may necessitate immediate dismissal. For additional information refer to the Employee Handbook; Policy 211 Employment – Performance Improvement/Conduct; and Policy 212 Employment – Termination of Employment*

## ADVERSE INFORMATION

The NISPOM requires that cleared defense contractor employees report to their FSO adverse information regarding any of their cleared employees. As a general rule, adverse information is that which reflects unfavorably on the trustworthiness or reliability of the employee and suggests that their ability to safeguard classified information may be impaired. Examples of this include: excessive indebtedness or recurring financial problems, unexplained affluence, use of illegal drugs (including marijuana even if legal in the State) or excessive use of intoxicants, bizarre behavior, mental or emotional problems, and criminal behavior. Wage garnishments

might be considered adverse information, check with your FSO to determine if reportable. Reports based on rumor or innuendo should not be made.

Reporting adverse information on coworkers is one of the most difficult tasks you may have. Employees find it difficult to be objective in assessing the impact of personal problems on job performance or continuing clearance eligibility. Many employees feel by reporting such behavior they are playing a policing role which they have no desire to perform. Other employees may take too zealously to this reporting requirement. Employees are cautioned against creating an atmosphere of suspicion or intrusiveness in the work place. Employees should be more concerned with their own work than that of others, but at the same time they should be vigilant and not turn a blind eye to the questionable behavior or practices of coworkers.

Employees found to have a problem with drugs or intoxicants will be processed in accordance with legal constraints, company policy and procedures relating to employee support.

Adverse information should be reported to protect the individual from being placed in a position where he or she could be exploited and persuaded to commit a security violation or even espionage. Many espionage cases can be cited in which hostile intelligence agents exploited a human weakness. If you are unsure if certain behavior requires reporting, you should consult your FSO for guidance.

## REQUIRED REPORTS

Cleared employees are required to report any information pertaining to the following events directly to the FSO (see NISPOM 1-302).

1. Adverse Information.
2. Suspicious Contacts.
3. Change in name, marital status, citizenship, and termination of employment.
4. Citizenship by Naturalization.
5. Employees Desiring Not to Perform on Classified Work.
6. Refusal by an employee to execute the SF312.
7. Unauthorized Receipt of Classified Material.
8. Loss, compromise or suspected compromise of classified information.

## OTHER REPORTING REQUIREMENTS

In addition to the above, employees are required to report any act of sabotage, possible sabotage, terrorism, espionage, attempted espionage and any subversive or suspicious activity. You are also encouraged to report any attempts to solicit classified information, any unauthorized persons on company property, disclosure of classified information to an unauthorized person, along with any other condition that would qualify as a security violation or which common sense would dictate as worth reporting.

## TERMINATION OF EMPLOYMENT

As a cleared employee, you have a responsibility to surrender all classified material in your possession to the Security Officer upon termination / separation. In addition, you must sign and date a Debriefing Form and return your badge prior to departure.

## STANDARD PRACTICE PROCEDURES (SPP)

The Security Office publishes a procedural manual, the SPP, which outlines the security procedures in greater detail. All cleared employees who handle classified material are requested to read the SPP. Please contact your Security Representative to request a copy.

Click here to enter your completion record: